In the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of the Claims

1-33. Canceled

34. (Currently Amended) A method of authenticating a hardware token for operation with a host, comprising:

retrieving a value X from a memory separate from [[a]] the hardware token, the memory accessible to an authenticating entity, the value X generated from a non-varying computer fingerprint F of a host and an identifier P securing access to the hardware token, wherein the fingerprint F is computed at least in part from non-varying host information C based on a unique characteristic of the host;

regenerating the same identifier P at least in part from the value X and the fingerprint F; and

transmitting the regenerated identifier P to the hardware token to authenticate the hardware token for operation with the host.

35. Canceled

36. (Previously Presented) The method of claim 34, wherein the fingerprint F is computed at least in part from the host information C and a non-varying server specific value V.

37. (Currently Amended) The method of ~~claim 34~~ claim 36, wherein the fingerprint F is computed at least in part from the host information C, [[a]] the non-varying server specific value V, and a non-varying string Z.

38. (Currently Amended) The method of claim 34, wherein the value X is computed in the hardware token.

39. (Original) The method of claim 34, wherein the value X is computed according to $X = f(P, F)$, wherein $f(P, F)$ is a reversible function such that $f(f(P, F), F) = P$.

40. (Original) The method of claim 39, wherein $f(P, F)$ comprises P XOR F.

41. (Original) The method of claim 34, wherein the value X is further computed at least in part from a user identifier U.

42. (Original) The method of claim 41, wherein the value X is computed according to $X = f(P, U, F)$, wherein $f(P, U, F)$ is a reversible function such that $f(f(P, U, F), U, F) = P$.

43. (Original) The method of claim 42, wherein $f(P, U, F)$ is P XOR U XOR F.

44. (Currently Amended) The method of claim 34, wherein:

the authenticating entity is the host computer, communicatively coupleable to the hardware token; and

the value X is stored in the host computer.

45-48. Canceled

49. (Currently Amended) An apparatus for authenticating a hardware token for operation with a host, comprising:

~~means for retrieving a value X from~~ a memory separate from [[a]] the hardware token, the memory accessible to an authenticating entity, the memory storing a value X, the value X generated from a non-varying computer fingerprint F of [[a]] the host and an identifier P securing access to the hardware token, wherein the fingerprint F is computed at least in part from non-varying host information C based on a unique characteristic of the host;

the host, adapted to:

compute the fingerprint F,

send the fingerprint F to the hardware token,

receive the value X from the hardware token, store the value X in the memory,

retrieve the value X from the memory,

regenerate ~~means for regenerating~~ the same identifier P at least in part from the retrieved value X and the fingerprint F~~; and means for transmitting~~, and

transmit the regenerated identifier P to the hardware token to authenticate the hardware token for operation with the host; and

the hardware token, adapted to:

receive the fingerprint F from the host,

generate the value X from the fingerprint F and the identifier P,

transmit the value X to the host for storage in the memory, and

receive the regenerated value P from the host, whereby the hardware token is authenticated for operation with the host.

50. Canceled

51. (Previously Presented) The apparatus of claim 49, wherein the fingerprint F is computed at least in part from the host information C and a non-varying server specific value V.

52. (Currently Amended) The apparatus of ~~claim 49~~ claim 51, wherein the fingerprint F is computed at least in part from the host information C, [[a]] the non-varying server specific value V, and a non-varying string Z.

53. (Currently Amended) The apparatus of claim 49, wherein the value X is computed in the hardware token.

54. (Original) The apparatus of claim 49, wherein the value X is computed according to $X = f(P, F)$,wherein $f(P, F)$ is a reversible function such that $f(f(P, F), F) = P$.

55. (Original) The apparatus of claim 54, wherein $f(P, F)$ comprises P XOR F.

56. (Original) The apparatus of claim 49, wherein the value X is further computed at least in part from a user identifier U.

57. (Original) The apparatus of claim 56, wherein the value X is computed according to $X = f(P, U, F)$,wherein $f(P, U, F)$ is a reversible function such that $f(f(P, U, F), U, F) = P$.

58. (Original) The apparatus of claim 57, wherein $f(P, U, F)$ is P XOR U XOR F.

59. (Currently Amended) The apparatus of claim 49, wherein:

the authenticating entity is the host computer, communicatively coupleable to the hardware token; and

the value X is stored in the host computer.

60-63. Canceled

64. (Previously Presented) An apparatus for authenticating a hardware token for operation with a host, the apparatus comprising a processor and a computer readable storage medium storing instructions for performing steps comprising:

retrieving a value X from a memory separate from [[a]] the hardware token, the memory accessible to an authenticating entity, the value X generated from a non-varying computer fingerprint F of a host and an identifier P securing access to the hardware token, wherein the fingerprint F is computed at least in part from non-varying host information C based on a unique characteristic of the host;

regenerating the same identifier P at least in part from the value X and the fingerprint F; and

transmitting the regenerated identifier P to the hardware token to authenticate the hardware token for operation with the host.

65. Canceled

66. (Previously Presented) The apparatus of claim 64, wherein the fingerprint F is computed at least in part from the host information C and a non-varying server specific value V.

67. (Currently Amended) The apparatus of ~~claim 64~~ claim 66, wherein the fingerprint F is computed at least in part from the host information C, [[a]] the non-varying server specific value V, and a non-varying string Z.

68. (Currently Amended) The apparatus of claim 64, wherein the value X is computed in the hardware token.

69. (Original) The apparatus of claim 64, wherein the value X is computed according to $X = f(P, F)$, wherein $f(P, F)$ is a reversible function such that $f(f(P, F), F) = P$.

70. (Original) The apparatus of claim 69, wherein $f(P, F)$ comprises P XOR F.

71. (Original) The apparatus of claim 64, wherein the value X is further computed at least in part from a user identifier U.

72. (Original) The apparatus of claim 71, wherein the value X is computed according to $X = f(P, U, F)$,wherein $f(P, U, F)$ is a reversible function such that $f(f(P, U, F), U, F) = P$.

73. (Original) The apparatus of claim 72, wherein $f(P, U, F)$ is P XOR U XOR F.

74. (Currently Amended) The apparatus of claim 64, wherein:

the authenticating entity is the host computer, communicatively coupleable to the hardware token; and

the value X is stored in the host computer.

75-78. Canceled